STATEWIDE INFORMATION SYSTEMS POLICY

Statewide Policy: Essential Information Security Roles

Effective Date: October 1, 2009

Approved: State of Montana Chief Information Officer

I. Purpose

This **Essential Information Security Roles Policy** (Policy) establishes the requirements to implement a computer security program based upon National Institute of Standards and Technology (NIST) guidance, specifically using the NIST risk management framework.

This Policy may conflict with other information system (IS) policies currently in effect. Where conflicts exist, the more restrictive policy governs. The development of future policies or standards will specifically identify and retire any superseded portions of current policies or standards.

II. Policy Statement

It is the policy of the State of Montana that agencies implement an Information System Security Program as outlined in National Institute Standards and Technology Special Publications 800-100, Revision 2 (NIST SP800-100) Information Security Handbook: A Guide for Managers, utilizing the Risk Management Framework outlined in National Institute Standards and Technology Special Publication 800-39 (NIST SP800-39) Managing Risk From Information Systems.

III. Applicability

This Policy is applicable to agencies, staff and all others, including outsourced third-parties (such as contractors, or other service providers), who have access to, use or manage information systems subject to the policy and standard provisions of §2-17-534, MCA. This Policy shall be communicated to staff and others who have access to or manage information, and information systems and assets.

IV. Scope

This Policy encompasses information systems for which agencies have administrative responsibility, including systems managed or hosted by third-parties on behalf of agencies.

V. Definitions

Agency Any entity of the executive branch, including the university system. Reference §2-17-506(8), MCA.

Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Reference 44 U.S.C., Sec. 3542.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Reference 44 U.S.C. Sec. 3502.
Information Resources	Information and related resources, such as personnel, equipment, funds, and information technology. Reference 44 U.S.C. Sec. 3502.
Information Technology	Hardware, software, and associated services and infrastructure used to store or transmit information in any form, including voice, video, and electronic data. Reference §2-17-506(7), MCA.

Refer to the Statewide Information system Policies and Standards Glossary for a list of local definitions.

Refer to the National Information Assurance (IA) Glossary, at http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf for common information systems security-related definitions.

VI. Authorizations, Roles, & Responsibilities

Refer to the Statewide Guidelines: Information Systems Security, paragraph II Authorizations, Roles, & Responsibilities for applicable authorization, roles, and responsibilities.

VII. Requirements

Agencies shall use NIST Special Publications 800-30, paragraph 2.3 (NIST SP800-30) Risk Management Guide for Information Technology Systems as general guidelines in assigning roles and responsibilities.

The same person identified and performing the duties as the agency information security manager required by §2-15-114(2), MCA may, at agency discretion, accomplish the Information Systems Security Officer responsibilities outlined in NIST SP800-30, paragraph 2.3; or the agency may separate the roles.

Distribution and assignment of roles and functions are individual agency implementation decision(s); however, responsibility and accountability for performance of the functions remains with the agency.

VIII. Compliance

Compliance with this Policy shall be evidenced by implementation and use of risk management processes and procedures aligned with NIST guidance, as referenced herein.

IX. Change Control and Exceptions

Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this instrument are made by submitting an Action Request form (at http://itsd.mt.govcontent/content/policy/policies/action_request.doc). Requests for exceptions are made by submitting an Exception Request form (at http://itsd.mt.gov/content/policy/policies/exception_request.doc). Changes to policies and standards will be prioritized and acted upon based on impact and need.

X. Closing

For questions or comments about this instrument, contact the State of Montana Chief Information Officer at ITSD Service Desk (at http://servicedesk.mt.gov/ess.do), or:

PO Box 200113
Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

XI. Cross-Reference Guide

A. State/Federal Laws/MOM

- §2-15-114, MCA. Security Responsibilities Of Departments For Data
- MOM 3-0130 Discipline

B. IT Procedures or Guidelines Supporting this Policy

- NIST SP800-100 Rev 2 Information Security Handbook: A Guide for Managers
- NIST SP800-39 Managing Risk From Information Systems
- NIST SP800-30, paragraph 2.3 Risk Management Guide for Information Technology Systems
- Statewide Policy: Establishing and Implementing Statewide Information Technology Policies and Standards
- Statewide Procedure: Establishing and Implementing Statewide Information Technology Policies and Standards

XII. Administrative Use

Product ID:	POL-20080714a
Proponent:	Chief Information Officer
Version:	1.0.2
Version Date:	2/17/2009
Approved Date:	February 17, 2009
Effective Date:	October 1, 2009
Change & Review Contact:	ITSD Service Desk (at http://servicedesk.mt.gov/ess.do)
Review Criteria:	Event Review: Any event affecting this policy may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	October 1, 2014
Last Review/Revision:	
Change Record:	